Queen Mary
University of London

MAS 305 — Algebraic Structures II

Notes 8 — **Autumn 2006**

Simple groups

Definition A nontrivial group G is *simple* if the only normal subgroups of G are $\{1_G\}$ and G. That is, a group is simple if it has precisely *two* normal subgroups.

If G is Abelian then all its subgroups are normal. Therefore, if it is nontrivial then either G is cyclic of prime order (and hence simple) or G is not simple.

If G is a nontrivial finite p-group for some prime p then it has normal subgroups of all orders dividing $|G|$. Hence either G is cyclic of prime order (and hence simple) or G is not simple.

If $|G| = 2p$ for an odd prime p then G is not simple, because it has a normal subgroup of order p.

If $G = S_n$ for $n \geqslant 3$ then G is not simple, because A_n is a nontrivial normal subgroup.

We have proved that if $20 \leqslant |G| \leqslant 24$ then G is not non-Abelian simple. In fact, it is true that if $2 \leqslant |G| \leqslant 59$ then G is not non-Abelian simple. Most cases can be dealt with using the techniques we used for the range 20–24.

Example If $|G| = 56$ then G has 1 or 8 Sylow 7-subgroups. If 1, then it is normal, so G is not simple. If 8, then there are $8 \times 6 = 48$ elements of order 7 (because such an element cannot be in more than one subgroup of order 7), leaving at most $56 - 48 = 8$ elements of orders dividing 8, so there can only be 1 Sylow 2-subgroup, so it is normal. Therefore G is not simple.

There is a non-Abelian simple group of order 60: the alternating group A_5. The remainder of this section proves that the alternating groups A_n are simple for $n \geqslant 5$.

Lemma Let $x \in A_n$. Then either

(a) $C_{S_n}(x) \leqslant A_n$ and the conjugacy class x^{S_n} splits up into two conjugacy classes of equal size in A_n; or

(b) $C_{S_n}(x)$ contains an odd permutation and x^{S_n} is a single conjugacy class in A_n.

Proof Write $C = C_{S_n}(x)$. Clearly $x^{A_n} \subseteq x^{S_n}$. Also, it is clear that either C contains an odd permutation or $C \leqslant A_n$.

(a) If $C \leqslant A_n$ then $\left|x^{A_n}\right| = |A_n : C| = |A_n| / |C| = \frac{1}{2}|S_n| / |C| = \frac{1}{2}|S_n : C| = \frac{1}{2}\left|x^{S_n}\right|$.

(b) We know that A_nC is a subgroup of S_n, because $A_n \lhd S_n$. If $C \nleqslant A_n$ then C contains an odd permutation and so A_nC is strictly larger than A_n, so $A_nC = S_n$. By the Third Isomorphism Theorem,

$$S_n/A_n = A_nC/A_n \cong C/A_n \cap C$$

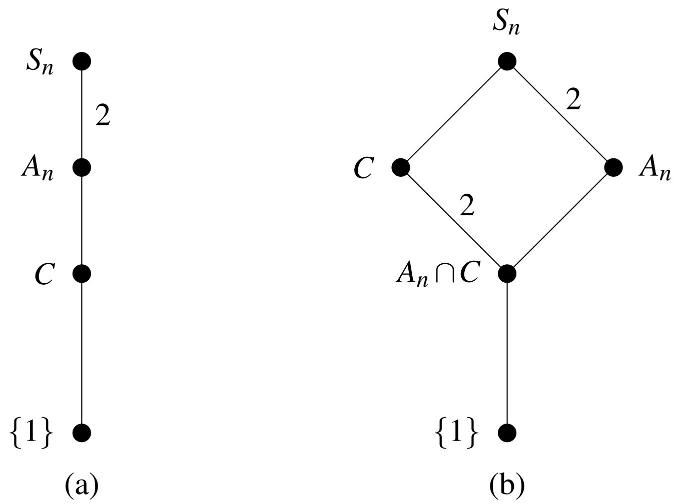
so

$$|C : A_n \cap C| = |S_n : A_n| = 2.$$

However, $A_n \cap C = C_{A_n}(x)$, so

$$\left|x^{A_n}\right| = |A_n : C_{A_n}(x)| = |A_n : A_n \cap C| = \frac{|A_n|}{|A_n \cap C|} = \frac{\frac{1}{2}|S_n|}{\frac{1}{2}|C|} = \frac{|S_n|}{|C|} = |S_n : C| = \left|x^{S_n}\right|.$$

Hence $x^{A_n} = x^{S_n}$. □



We can use this lemma to see how the conjugacy classes of S_5 behave in A_5.

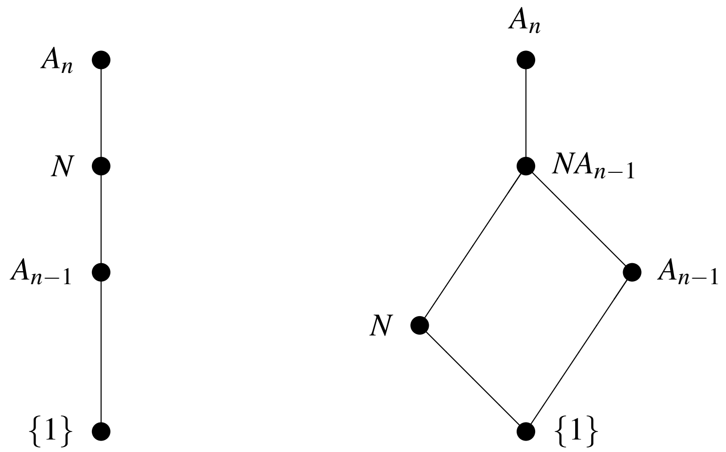
x	$\lvert x^{S_5}\rvert$	odd permutation in $C(x)$?	size of conjucacy class(es) in A_5
$(1\,2\,3\,4\,5)$	24	no	$12+12$
$(1\,2\,3)$	20	$(4\,5)$	20
$(1\,2)(3\,4)$	15	$(1\,2)$	15
(1)	1	yes	1
	60		

The only partial sums of 12, 12, 20, 15 and 1 which contain 1 and divide 60 are 1 and 60. Therefore A_5 is simple.

Theorem The alternating group A_n is simple if $n \geqslant 5$.

Proof We use induction on n. We have shown that A_5 is simple, so we assume that $n \geqslant 6$ and A_{n-1} is simple.

Let $N \trianglelefteq A_n$. Then $N \cap A_{n-1} \trianglelefteq A_{n-1}$. By the inductive hypothesis, $N \cap A_{n-1} = \{1\}$ or $N \cap A_{n-1} = A_{n-1}$, that is, $N \geqslant A_{n-1}$.



(a) (b)

(a) Suppose that $N \geqslant A_{n-1}$. Write $G = A_n$, and let α be the point fixed by A_{n-1}. Then $G_\alpha \leqslant N$ so $N_\alpha = G_\alpha \cap N = G_\alpha$. Since $N \geqslant A_{n-1}$, the orbits of N are unions of orbits of A_{n-1}. The orbits of A_{n-1} have sizes 1 and $n-1$ (because $n \geqslant 4$), so either $\lvert\alpha^N\rvert = 1$ or $\lvert\alpha^N\rvert = n$. By the Orbit-Stabilizer Theorem, $\lvert N : N_\alpha\rvert = 1$ or n. If $\lvert N : N_\alpha\rvert = 1$ then $N = N_\alpha = G_\alpha = A_{n-1}$. But the conjugates of G_α are the other point-stabilizers, which are not contained in G_α, so $A_{n-1} \not\trianglelefteq A_n$, so $N \neq A_{n-1}$. If $\lvert N : N_\alpha\rvert = n$ then $\lvert N\rvert = n \times \lvert N_\alpha\rvert = n \times \lvert A_{n-1}\rvert = \lvert A_n\rvert$ so $N = A_n$.

(b) Suppose that $N \cap A_{n-1} = \{1\}$. Because $N \trianglelefteq A_n$, we know that NA_{n-1} is a subgroup of A_n. By the Third Isomorphism Theorem,

$$NA_{n-1}/N \cong A_{n-1}/N \cap A_{n-1} = A_{n-1}/\{1\} \cong A_{n-1},$$

so $|NA_{n-1}|/|N| = |A_{n-1}|$ and so $|N| = |NA_{n-1}|/|A_{n-1}| \leqslant |A_n|/|A_{n-1}| = n$. Therefore if $x \in N \setminus \{1\}$ then $\left|x^{A_n}\right| \leqslant n-1$, because $x^{A_n} \subseteq N$ and the identity is a whole conjugacy class. By the lemma, $\left|x^{S_n}\right| \leqslant 2(n-1)$.

Suppose that $x \in N \setminus \{1\}$. Then no conjugate of x is in G_α, so all cycles of x have length at least 2. If $g \in C(x)$ then $\beta x^r g = \beta g x^r$ for all points β and all positive integers r, so once βg is known than γg is known for all γ in the same cycle of x as β. Therefore, if x has a single cycle then $|C(x)| \leqslant n$ and so $\left|x^{S_n}\right| \geqslant (n-1)! > 2(n-1)$ when $n \geqslant 5$. Otherwise, suppose that x has two cycles of lengths m_1 and m_2 (and possibly others). Then $|C(x)| \leqslant n \times (n-m_1) \times (n-m_1-m_2)!$ so

$$\left|x^{S_n}\right| \geqslant (n-1) \times \cdots \times (n-m_1+1) \times (n-m_1-1) \times \cdots \times (n-m_1-m_2+1).$$

If $m_1 = 2$ then $\left|x^{S_n}\right| \geqslant (n-1)(n-3) \geqslant 3(n-1)$ when $n \geqslant 6$; while if $m_1 > 2$ then $\left|x^{S_n}\right| \geqslant (n-1)(n-2) \geqslant 4(n-1)$ when $n \geqslant 6$. So there can be no element x in $N \setminus \{1\}$, so $N = \{1\}$. $\square$